

On codes in the projective linear group $\text{PGL}(2, q)$

Tao Feng^a, Weicong Li^a, Jingkun Zhou^{a,*}

^a*School of Mathematical Sciences, Zhejiang University, 38 Zheda Road, Hangzhou 310027, Zhejiang P.R. China*

Abstract

In this paper, we resolve a conjecture of Green and Liebeck [Disc. Math., 343 (8):117119, 2019] on codes in $\text{PGL}(2, q)$. To be specific, we show that: if D is a dihedral subgroup of order $2(q + 1)$ in $G = \text{PGL}(2, q)$, and $A = \{g \in G : g^{q+1} = 1, g^2 \neq 1\}$, then $\lambda G = A \cdot D$, where $\lambda = q$ or $q - 1$ according as q is even or odd.

Keywords: codes, Cayley graphs, projective linear groups, linearized polynomials.
Mathematics Subject Classification (2010): 05C25 94B60 11T06

1. Introduction

Let G be a finite group, A be a nonempty proper subset of G and λ be a natural number. Following [11], we say that A divides λG if there is a subset B of G such that the multiset $\{ab : a \in A, b \in B\}$ covers each element of G exactly λ times; the subset B is called a *code* with respect to A and we write $A \cdot B = \lambda G$. If the subset A of G does not contain the identity and satisfies that $A = \{g^{-1} : g \in A\}$, we define the *Cayley graph* $\text{Cay}(G, A)$ as the graph with vertex set G and edge set $\{(g, h) : g^{-1}h \in A\}$. In such a case, $A \cdot B = \lambda G$ implies that the code B is a collection of vertices of $\text{Cay}(G, A)$ such that each vertex has exactly λ neighbors in B . If $\lambda = 1$, then B is called a *perfect code* of $\text{Cay}(G, A)$. This notion of perfect codes generalizes the classical perfect codes in coding theory. The recent paper [6] gives a very nice exposition of their relationship and the history of research development in this direction. We refer the reader to [1, 12, 8] for the classical theory of perfect codes over graphs and [6, 5, 10, 2] for some recent progress.

When A is the union of conjugacy classes, it is of particular interest to study codes in $\text{Cay}(G, A)$. In [4, 11], the authors use representation theory to study such codes. However, there are very few known examples in the literature, and this motivated the authors of [5] to study the case where A is a union of conjugacy classes and B is a subgroup. They construct several families of such codes in symmetric groups and special linear groups $\text{SL}(2, q)$ and pose two conjectured families. This paper resolves their Conjecture 3.2, which we now state as a theorem.

*Corresponding author

Email addresses: tfeng@zju.edu.cn (Tao Feng), conglw@zju.edu.cn (Weicong Li), jingkunz@zju.edu.cn (Jingkun Zhou)

Theorem 1.1. *Let $G = \text{PGL}(2, q)$ and D be a dihedral subgroup of order $2(q+1)$. Set*

$$A = \{g \in G : g^{q+1} = 1, g^2 \neq 1\}.$$

Then $\lambda G = A \cdot D$, where $\lambda = q$ or $q-1$ according as q is even or odd.

This paper is organized as follows. In Section 2, we describe the model of $\text{GL}(2, q)$ that we use and present some preliminary results about the preimages of A and D in $\text{GL}(2, q)$, where A, D are the subsets in Theorem 1.1. We shall prove the theorem by working inside $\text{GL}(2, q)$. In Section 3, we present the proof of Theorem 1.1, which is divided into a series of technical lemmas.

2. Preliminaries

Let q be a prime power, and \mathbb{F}_{q^2} be a finite field with q^2 elements. We regard \mathbb{F}_{q^2} as a vector space V of dimension 2 over \mathbb{F}_q . Let $f : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$ be an \mathbb{F}_q -linear transformation. There exists a unique polynomial $F(X) = aX + bX^q \in \mathbb{F}_{q^2}[X]$ such that $f(x) = F(x)$ for all $x \in \mathbb{F}_{q^2}$, cf. [9, Chapter 3]. Such a polynomial $F(X)$ is a *reduced q -linearized polynomial*, i.e., $\deg(F) \leq q^2 - 1$ and the transformation $x \mapsto F(x)$ over \mathbb{F}_{q^2} is \mathbb{F}_q -linear.

Lemma 2.1. *For $a, b \in \mathbb{F}_{q^2}$, the \mathbb{F}_q -linear transformation $x \mapsto ax + bx^q$ over \mathbb{F}_{q^2} is invertible if and only if $a^{q+1} \neq b^{q+1}$.*

Proof. The case where one of a, b is zero is trivial, so we assume that $ab \neq 0$. By [9, Lemma 7.1], the linear transformation $x \mapsto ax + bx^q$ over \mathbb{F}_{q^2} is invertible if and only if $ax + bx^q = 0$ has no nonzero root in \mathbb{F}_{q^2} . For $x \in \mathbb{F}_{q^2}^*$, $ax + bx^q = 0$ if and only if $x^{q-1} = -ab^{-1}$. The latter equation has a solution if and only if $(-ab^{-1})^{q+1} = 1$, i.e., $a^{q+1} = b^{q+1}$. The claim now follows. \square

By Lemma 2.1, the set of invertible \mathbb{F}_q -linear transformations of $V = \mathbb{F}_{q^2}$, i.e., $\text{GL}(V)$, consists of the transformations of the form

$$f_{a,b} : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}, \quad x \mapsto ax + bx^q, \quad (2.1)$$

where $a, b \in \mathbb{F}_{q^2}$ such that $a^{q+1} \neq b^{q+1}$.

Lemma 2.2. *Suppose that $a, b \in \mathbb{F}_{q^2}$ such that $a^{q+1} \neq b^{q+1}$, and let $f_{a,b}$ be as in (2.1). The inverse transformation f^{-1} is $f_{a',b'}$, where*

$$a' = \frac{a^q}{a^{q+1} - b^{q+1}}, \quad b' = \frac{-b}{a^{q+1} - b^{q+1}}.$$

Proof. This follows by direct check, and we omit the details. \square

Take an element $t \in \mathbb{F}_{q^2}^*$. For $f_{c,d} \in \text{GL}(V)$, we compute that

$$\begin{aligned} f_{c,d}^{-1}(f_{t,0}(f_{c,d}(x))) &= \frac{1}{c^{q+1} - d^{q+1}} (c^q(tcx + tdx^q) - d(tcx + tdx^q)^q) \\ &= \frac{tc^{q+1} - t^q d^{q+1}}{c^{q+1} - d^{q+1}} x + \frac{c^q d(t - t^q)}{c^{q+1} - d^{q+1}} x^q, \end{aligned} \quad (2.2)$$

where we used Lemma 2.2 in the first equality. If $d = 0$, then it equals $f_{t,0}(x)$. If $d \neq 0$, we write $s := cd^{-1}$, so that $f_{c,d}^{-1}(f_{t,0}(f_{c,d}(x))) = L_{t,s}(x)$, where

$$L_{t,s}(x) := \frac{ts^{q+1} - t^q}{s^{q+1} - 1}x + \frac{(t - t^q)s^q}{s^{q+1} - 1}x^q. \quad (2.3)$$

Here, we have $s^{q+1} \neq 1$ by Lemma 2.1. In particular, we have $L_{t,0}(x) = t^q x$. To be consistent, we write

$$L_{t,\infty}(x) := tx, \quad \text{i.e., } L_{t,\infty} = f_{t,0}. \quad (2.4)$$

Lemma 2.3. *For $t \in \mathbb{F}_{q^2}^*$, the conjugacy class of $\text{GL}(V)$ containing $L_{t,\infty} = f_{t,0}$ is $C_t := \{L_{t,s} : s \in S'\}$, where $S' = \{u \in \mathbb{F}_{q^2} : u^{q+1} \neq 1\} \cup \{\infty\}$. If $t \notin \mathbb{F}_q$, then $C_t = C_{t^q}$ and $|C_t| = q(q-1)$.*

Proof. The first part has been established in the preceding arguments. Assume that $t \notin \mathbb{F}_q$. We have $L_{t,0}(x) = t^q x$, which is in the conjugacy class C_t and also equals $L_{t^q,\infty}$, so $C_t = C_{t^q}$. For $s \in \mathbb{F}_{q^2}^*$ with $s^{q+1} \neq 1$, the two transformations $L_{t,s}$ and $L_{t,\infty}$ are distinct since they have different degrees. Also, $L_{t,0} \neq L_{t,\infty}$, since $t \notin \mathbb{F}_q$. We deduce from the preceding arguments that the stabilizer of $L_{t,\infty}$ under the action of $\text{GL}(V)$ via conjugation is $\{f_{c,0} : c \in \mathbb{F}_{q^2}^*\}$. Therefore,

$$|C_t| = \frac{|\text{GL}(V)|}{q^2 - 1} = \frac{(q^2 - 1)(q^2 - q)}{q^2 - 1} = q(q - 1).$$

□

Lemma 2.4. *For $g \in \text{GL}(V)$ with $V = \mathbb{F}_{q^2}$, its quotient image \bar{g} in $\text{PGL}(V)$ is in the set A in Theorem 1.1 if and only if it is conjugate to $f_{t,0}$ in $\text{GL}(V)$ for some element $t \in \mathbb{F}_{q^2}^*$ such that $t^{2(q-1)} \neq 1$.*

Proof. Take $g \in \text{GL}(V)$ such that $\bar{g} \in A$, i.e., $\bar{g}^{q+1} = 1$, $\bar{g}^2 \neq 1$. Then g^{q+1} is the scalar multiplication by some $\lambda \in \mathbb{F}_q^*$. In particular, $g^{q^2-1} = 1$. In this proof, we regard g as a 2×2 matrix over \mathbb{F}_q by specifying a basis of $V = \mathbb{F}_{q^2}$ over \mathbb{F}_q . Let $m(X)$ be the minimal polynomial of the matrix g , which lies in $\mathbb{F}_q[X]$. Since $g^{q^2-1} = 1$, we have $m(X) | X^{q^2-1} - 1$. Since $X^{q^2-1} - 1$ has no repeated roots, so does $m(X)$. Also, by the Cayley-Hamilton Theorem, we have $m(g) = 0$.

We claim that $m(X)$ is an irreducible polynomial of degree 2 over \mathbb{F}_q . If $m(X)$ has degree 1, then g is a scalar matrix, and $\bar{g} = 1$, which is impossible. If $m(X)$ has two roots λ_1, λ_2 in \mathbb{F}_q , then $\lambda_1 \neq \lambda_2$ by the previous paragraph and so g is conjugate to the diagonal matrix $\text{diag}(\lambda_1, \lambda_2)$ in $\text{GL}(V)$. Since g^{q+1} is a scalar matrix, so should be $\text{diag}(\lambda_1^{q+1}, \lambda_2^{q+1})$. We thus have $\lambda_1^2 = \lambda_2^2$, i.e., $\lambda_1 = \pm \lambda_2$. This leads to a contradiction that $\bar{g}^2 = 1$, and thus the claim follows.

Write $m(X) = X^2 + cX + d$ with $c, d \in \mathbb{F}_q$, and let t be a root of $m(X)$ in \mathbb{F}_{q^2} . Then $t \notin \mathbb{F}_q$, and $m(X) = (X - t)(X - t^q)$. Set $v := g(1)$. We claim that $v \notin \mathbb{F}_q$: otherwise, $g(1) = v \cdot 1$ and v is an eigenvalue of g , so $m(v) = 0$, contradicting the irreducibility of $m(X)$. We have $g(g(1)) + cg(1) + d = 0$, so $g(v) = -d - cv$. Therefore, $(g(1), g(v)) = (1, v)M$ with $M = \begin{pmatrix} 0 & -d \\ 1 & -c \end{pmatrix}$. It is routine to check $(f_{t,0}(1), f_{t,0}(t)) = (1, t)M$. Let h be

the element of $\text{GL}(V)$ that maps the ordered basis $(1, t)$ to $(1, v)$. Then g is mapped to $f_{t,0}$ by h via conjugation, i.e., g is in the conjugacy class of $f_{t,0}$ in $\text{GL}(V)$.

We claim that $t^{2(q-1)} \neq 1$. Otherwise, $t^2 \in \mathbb{F}_q^*$ and $X^2 - t^2$ is the minimal polynomial of t over \mathbb{F}_q . It follows that $m(X) = X^2 - t^2$. Hence $g(g(x)) = t^2x$, and $\bar{g}^2 = 1$: a contradiction. This proves the necessity part of the lemma.

For the sufficient part, it suffices to verify that $\overline{f_{t,0}}^{q+1} = 1$ and $\overline{f_{t,0}}^2 \neq 1$ provided that $t^{2(q-1)} \neq 1$. This is clear since $f_{t,0}^{q+1}(x) = t^{q+1}x$, $f_{t,0}^2(x) = t^2x$, and t^{q+1} is in \mathbb{F}_q^* while t^2 is not under the assumption on t . This completes the proof. \square

The following is an immediate corollary.

Corollary 2.5. *Let A be the set as in Theorem 1.1, regard \mathbb{F}_{q^2} as a 2-dimensional vector space over \mathbb{F}_q so that $\text{GL}(2, q) = \text{GL}(V)$. Then the full preimage of A in $\text{GL}(V)$ is the set $\tilde{A} := \cup_{t \in T} C_t$, where $T = \{t \in \mathbb{F}_{q^2}^* : t^{2(q-1)} \neq 1\}$.*

Lemma 2.6. *Take the same notation as in Lemma 2.3. For $t, t' \in \mathbb{F}_{q^2}^*$, we have $C_t = C_{t'}$ if and only if $t' = t$ or $t' = t^q$.*

Proof. We have $C_t = C_{t^q}$ by Lemma 2.3. The minimal polynomial of the \mathbb{F}_q -linear transformation $f_{t,0}$ is $X - t$ or $(X - t)(X - t^q)$ according as t is in \mathbb{F}_q or not, as we showed in the proof of Lemma 2.4. Since conjugate transformations has the same minimal polynomial, the claim now follows. \square

We shall need the following technical lemma in the next section.

Lemma 2.7. *Suppose that q is odd, and let x_0 be a root of $F(x) = cx^2 + dx + c^q$, where $c \in \mathbb{F}_{q^2}^*$, $d \in \mathbb{F}_q^*$. Then $x_0^{q+1} = 1$ if and only if $\Delta_F = d^2 - 4c^{q+1}$ is zero or a nonsquare in \mathbb{F}_q .*

Proof. Take $r \in \mathbb{F}_{q^2}^*$ such that $r^2 = \Delta_F$. This is possible since Δ_F is in \mathbb{F}_q . We solve that $x_0 = \frac{-d + \epsilon r}{2c}$ for some $\epsilon = \pm 1$, so

$$(2c)^{q+1} x_0^{q+1} = (-d + \epsilon r)(-d + \epsilon r^q) = d^2 - d\epsilon(r + r^q) + r^{q+1}.$$

We consider three separate cases.

- (1) If $\Delta_F = 0$, then $4c^{q+1} = d^2$, $r = 0$, and $4c^{q+1}x_0^{q+1} = d^2$, so $x_0^{q+1} = 1$.
- (2) If Δ_F is a nonsquare in \mathbb{F}_q^* , then the minimal polynomial of r over \mathbb{F}_q is $X^2 - \Delta_F$, and so $r^q + r = 0$, $r^{q+1} = -\Delta_F$. In this case, $4c^{q+1}x_0^{q+1} = d^2 - \Delta_F = 4c^{q+1}$, and we have $x_0^{q+1} = 1$.
- (3) If Δ_F is a square in \mathbb{F}_q^* , then $r \in \mathbb{F}_q^*$. In this case, $4c^{q+1}x_0^{q+1} = d^2 - 2d\epsilon r + r^2$. If $x_0^{q+1} = 1$, then we deduce that $-2d\epsilon r + 2r^2 = 0$, i.e., $d\epsilon = r$. It follows that $d^2 = r^2 = d^2 - 4c^{q+1}$, yielding $c = 0$: a contradiction. Hence $x_0^{q+1} \neq 1$ in this case.

This completes the proof. \square

3. Proof of Theorem 1.1

This section is devoted to the proof of Theorem 1.1, which is divided into a series of lemmas. We regard \mathbb{F}_{q^2} as a two-dimensional vector space V over \mathbb{F}_q , and identify $\text{GL}(2, q)$ with $\text{GL}(V)$. The cases $q = 2, 3$ of Theorem 1.1 can be directly verified by computer, so we assume that $q > 3$ in the sequel. We introduce the following subset of $\text{GL}(V)$:

$$\tilde{D} := \{f_{t,0}, f_{0,t} : t \in \mathbb{F}_{q^2}^*\},$$

where $f_{a,b}$ is as in (2.1). It is a subgroup of order $2(q^2 - 1)$, and its quotient image in $\text{PGL}(V)$ is a dihedral subgroup D of order $2(q + 1)$. When $q > 3$, there is exactly one conjugacy class of dihedral subgroups of order $2(q + 1)$ in $\text{PGL}(2, q)$, cf. [3, 7]. We can thus take this D as the one in Theorem 1.1.

It is convenient to introduce the following notation:

$$S := \{s \in \mathbb{F}_{q^2}^* : s^{q+1} \neq 1\}, \quad (3.1)$$

$$T := \{t \in \mathbb{F}_{q^2}^* : t^{2(q-1)} \neq 1\}. \quad (3.2)$$

We have $\mathbb{F}_q^* \cap T = \emptyset$, and $|T| = (q^2 - 1) - (q - 1) = q(q - 1)$ or $|T| = (q^2 - 1) - 2(q - 1) = q(q - 1)$ according as q is even or odd. The full preimage \tilde{A} of the set A in Theorem 1.1 is the union of conjugacy class C_t 's by Corollary 2.5, where t ranges over T . Let T_1 be a subset of T such that it contains exactly one element of $\{t, t^q\}$ for each $t \in T$. Then $|T_1| = \frac{1}{2}|T|$, and \tilde{A} is the disjoint union of C_t 's with $t \in T_1$ by Lemma 2.6.

We now reformulate Theorem 1.1 in terms of $\text{GL}(V)$. To show that $A \cdot D = \lambda \cdot \text{PGL}(2, q)$, where $\lambda = q$ or $q - 1$ according as q is even or odd, it suffices to show that $\tilde{A} \cdot \tilde{D} = |T| \cdot \text{GL}(V)$. Recall that the conjugacy class C_t consists of $L_{t,s}$'s with $s \in S \cup \{0\} \cup \{\infty\}$, cf. (2.3) and (2.4).

Lemma 3.1. *For $s \in S$, $t \in T$ and $r \in \mathbb{F}_{q^2}^*$, if $f_{a,b} = L_{t,s} \cdot f_{r,0}$ or $f_{a,b} = L_{t,s} \cdot f_{0,r}$, then $ab \neq 0$.*

Proof. We have $L_{t,s}(f_{r,0}(x)) = \frac{(ts^{q+1}-t^q)r}{s^{q+1}-1}x + \frac{(t-t^q)s^q r^q}{s^{q+1}-1}x^q$. If the coefficient of x is zero, then $ts^{q+1} = t^q$, i.e., $t^{q-1} = s^{q+1}$. We deduce that $t^{(q-1)^2} = 1$. Since $t^{q^2-1} = 1$, we deduce that $t^{2(q-1)} = t^{q^2-1-(q-1)^2} = 1$, a contradiction to $t \in T$. If the coefficient of x^q is zero, then $t = t^q$, i.e., $t^{q-1} = 1$, which is again a contradiction to $t^{2(q-1)} \neq 1$. The case of $f_{a,b} = L_{t,s} \cdot f_{0,r}$ is similar, and we omit the details. \square

Lemma 3.2. *For $f_{a,b} \in \text{GL}(V)$ with $ab = 0$, its multiplicity in $\tilde{A} \cdot \tilde{D}$ is $|T|$, which is $q(q - 1)$ or $(q - 1)^2$ according as q is even or odd.*

Proof. We consider only the case $f_{a,0}$ with $a \in \mathbb{F}_{q^2}^*$, and the case of $f_{0,b}$ with $b \in \mathbb{F}_{q^2}^*$ is similar. By Lemma 3.1, it suffices to consider the number of ways to express $f_{a,0}$ in the form $L_{t,0} \cdot g$ with $g \in \tilde{D}$, $t \in T_1$.

- (1) If $s = \infty$, $L_{t,\infty}(f_{r,0}(x)) = trx$, $L_{t,\infty}(f_{0,r}(x)) = trx^q$.
- (2) If $s = 0$, then $L_{t,0}(f_{r,0}(x)) = t^q rx$, $L_{t,0}(f_{0,r}(x)) = t^q rx^q$.

We recall that $t \neq t^q$ for $t \in T$. For each $t \in T_1$, we have $f_{a,0} = L_{t,\infty} \cdot f_{at^{-1},0} = L_{t,0} \cdot f_{at^{-q},0}$. This gives $2|T_1|$ different expressions of $f_{a,0}$. This completes the proof. \square

It remains to consider the multiplicity of $f_{a,b}$ in $\tilde{A} \cdot \tilde{D}$, where $f_{a,b} \in GL(V)$ with $ab \neq 0$. By Lemma 3.1 and the proof of Lemma 3.2, it equals the number of $(s, t, r) \in S \times T_1 \times \mathbb{F}_{q^2}^*$ such that $L_{t,s} \cdot f_{r,0} = f_{a,b}$ or $L_{t,s} \cdot f_{0,r} = f_{a,b}$. By comparing the coefficients of x and x^q , the two equations are equivalent to

$$a = \frac{(ts^{q+1} - t^q)r}{s^{q+1} - 1}, \quad b = \frac{(t - t^q)s^q r^q}{s^{q+1} - 1}, \quad (3.3)$$

and

$$b = \frac{(ts^{q+1} - t^q)r}{s^{q+1} - 1}, \quad a = \frac{(t - t^q)s^q r^q}{s^{q+1} - 1}, \quad (3.4)$$

respectively. Observe that (3.4) can be obtained from (3.3) by switching a, b . We analyze (3.3) in the sequel, and the conclusions hold for (3.4) by interchanging a, b . We deduce from (3.3) that

$$t = ar^{-1} - br^{-q}s^{-q}, \quad t^q = ar^{-1} - br^{-q}s. \quad (3.5)$$

Raising the expression of t to q -th power and comparing with that of t^q , we deduce that s is a root of the quadratic equation

$$brX^2 + (a^q r - ar^q)X - (br)^q = 0. \quad (3.6)$$

Lemma 3.3. *The quadratic equation (3.6) has all its roots in $\mathbb{F}_{q^2}^*$.*

Proof. If q is odd, its discriminant $\Delta = (a^q r - ar^q)^2 + 4(br)^{q+1}$ lies in \mathbb{F}_q upon direct check, so the square roots of Δ and correspondingly the roots of (3.6) lie in \mathbb{F}_{q^2} . If q is even, we can rewrite the equation as $Y^2 + (a^q r + ar^q)Y + (br)^{q+1} = 0$, where $Y = brX$. The latter equation has coefficients in \mathbb{F}_q , so its roots lie in \mathbb{F}_{q^2} . This completes the proof. \square

Lemma 3.4. *If $s \in S$ is a root of (3.6), then*

- (1) s^{-q} is also a root and $s + s^{-q} = -b^{-1}a^q + b^{-1}ar^{q-1}$, $s^{1-q} = (br)^{q-1}$.
- (2) *If the values of t corresponding to s and s^{-q} as in (3.5) are in T , then exactly one of them is in T_1 .*

Proof. (1) Suppose $brs^2 + (a^q r - ar^q)s - (br)^q = 0$. Raising both sides to the q -th power and then multiplying both sides by $-s^{-2q}$, we get $-(br)^q + (a^q r - ar^q)s^{-q} + brs^{-2q} = 0$. The first claim now follows. Since $s \in S$, we have $s \neq s^{-q}$ and they are the two distinct roots of (3.6). The second claim then follows from Viète Theorem.

(2) Let $t_1 = ar^{-1} - br^{-q}s^{-q}$ and $t_2 = ar^{-1} - br^{-q}s$ be the two corresponding values of t . Then $t_1^q = t_2$ by (3.5). The claim now follows. \square

Lemma 3.5. *Take $(s, t, r) \in S \times \mathbb{F}_{q^2}^* \times \mathbb{F}_{q^2}^*$ such that (3.3) holds. If q is even, then $t \in T$; if q is odd, then $t \in T$ if and only if $r^{q-1} + a^{q-1} \neq 0$.*

Proof. Recall that $t \notin T$ if and only if $t^2 \neq t^{2q}$, cf. (3.2). From (3.5) we deduce that

$$\begin{aligned} t^{2q} - t^2 &= (ar^{-1} - br^{-q}s)^2 - (ar^{-1} - br^{-q}s^{-q})^2 \\ &= -2abr^{-q-1}s + b^2r^{-2q}s^2 + 2abr^{-q-1}s^{-q} - b^2r^{-2q}s^{-2q} \\ &= br^{-q}(s - s^{-q})(-2ar^{-1} + br^{-q}(s + s^{-q})). \end{aligned}$$

Since $s^{q+1} \neq 1$, i.e., $s \neq s^{-q}$, we see that $t^{2q} - t^2 = 0$ iff $-2ar^{-1} + br^{-q}(s + s^{-q}) = 0$. This does not hold if q is even, so t is in T in this case. If q is odd, then $-2ar^{-1} + br^{-q}(s + s^{-q}) = -ar^{-q}(r^{q-1} + a^{q-1})$ by Lemma 3.4, and the claim follows in this case. \square

By Lemma 3.3 and Lemma 3.4, for an element $r \in \mathbb{F}_{q^2}^*$ the two roots of (3.6) are either both in S or both in $\mathbb{F}_{q^2}^* \setminus S$, and in the former case the two roots are distinct. Set

$$R_1 := \{r \in \mathbb{F}_{q^2}^* : (3.6) \text{ has no roots in } S\}, \quad (3.7)$$

$$R_2 := \{r \in \mathbb{F}_{q^2}^* : (3.6) \text{ has two roots in } S\}. \quad (3.8)$$

The two subsets R_1 and R_2 form a partition of $\mathbb{F}_{q^2}^*$.

Lemma 3.6. *Suppose that q is odd and $r^{q-1} + a^{q-1} = 0$. Then $r \in R_2$ if and only if $\kappa(b, a) := -1 + b^{q+1}/a^{q+1}$ is a nonzero square in \mathbb{F}_q .*

Proof. We multiply both sides of (3.6) by $r^{-1}a$ and substitute $r^{q-1} = -a^{q-1}$ to obtain $baX^2 + 2a^{q+1}X + (ba)^q = 0$. Its discriminant is $\Delta = 4a^{2q+2}\kappa(b, a)$. By Lemma 2.7 and the preceding remark, its roots lie in S if and only if Δ is a nonzero square in \mathbb{F}_q . This completes the proof. \square

Lemma 3.7. *Take notation as above, and set $\kappa(a, b) := 1 - a^{q+1}/b^{q+1}$.*

- (1) *If q is odd and $\kappa(a, b)$ is a nonsquare in \mathbb{F}_q^* , then $|R_1| = \frac{(q-1)(q+3)}{2}$, $|R_2| = \frac{(q-1)^2}{2}$;*
- (2) *If q is odd and $\kappa(a, b)$ is a square in \mathbb{F}_q^* , then $|R_1| = |R_2| = \frac{q^2-1}{2}$;*
- (3) *If q is even, then $|R_1| = \frac{(q+2)(q-1)}{2}$, $|R_2| = \frac{q(q-1)}{2}$.*

Proof. Suppose that s is an element of $\mathbb{F}_{q^2}^*$ such that $s^{q+1} = 1$ and it is a root of (3.6) for some $r \in \mathbb{F}_{q^2}^*$. Then we have $bs^2 + a^q s = (as + b^q)r^{q-1}$. Since $a^{q+1} \neq b^{q+1}$ and $s^{q+1} = 1$, we deduce that $as + b^q \neq 0$. Similarly, $a + b^q s^q \neq 0$. Hence, r^{q-1} equals

$$\frac{bs^2 + a^q s}{as + b^q} = (a + b^q s^q)^{q-1}. \quad (3.9)$$

Therefore, $|R_1| = (q-1)|Y|$, where $Y := \{\frac{bs^2+a^q s}{as+b^q} : s^{q+1} = 1\}$, and $|R_2| = q^2 - 1 - |R_1|$. We note that Y consists of $(q-1)$ -st powers by (3.9), i.e., $c^{q+1} = 1$ for $c \in Y$.

We write Y' for the multiset of size $q+1$ corresponding to Y . Each element $c \in Y'$ has multiplicity 1 or 2, since

$$bX^2 + a^q X = c(aX + b^q) \quad (3.10)$$

has at most two solutions. Let n_i be the number of elements with multiplicity i in Y' for $i = 1, 2$. Then $n_1 + 2n_2 = q+1$, $|Y| = n_1 + n_2$. It remains to determine n_1 .

We claim that c has multiplicity 1 in Y' if and only if (3.10) has a repeated root. Suppose that (3.10) has two distinct roots s, s' for some $c \in Y$ and s such that $s^{q+1} = 1$. Then $ss' = -cb^{q-1}$ by Viète Theorem. By raising to the $(q+1)$ -st power, we deduce that $s'^{q+1} = 1$, and so c has multiplicity 2 in Y' . Conversely, suppose that (3.10) has a repeated root s . Since each element of Y' is a $(q-1)$ -st power, we write $c = z^{q-1}$ for some $z \in \mathbb{F}_{q^2}^*$. Take $\delta \in \mathbb{F}_{q^2}$ such that $\delta^q + \delta = 0$. Multiplying both sides of (3.10) by δz , we obtain $(bz\delta)X^2 + \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a^q z\delta)X + (bz\delta)^q = 0$. If q is odd, then $s^{q+1} = 1$ by Lemma 2.7. If q is even, the coefficient $a^q - ac$ of X in (3.10) equals 0 since the equation has a

repeated root. Thus (3.10) has the form $X^2 = cb^{q-1} = (zb)^{q-1}$, so the repeated root s satisfies $s^{q+1} = 1$. This proves the claim.

To summarize, the elements that have multiplicity 1 in Y' are those $c \in \mathbb{F}_{q^2}^*$ such that c is a $(q-1)$ -st power and (3.10) has a repeated root.

Suppose that q is odd. The equation (3.10) has a repeated root if and only if its determinant $\Delta_c := (a^q - ca)^2 + 4cb^{1+q}$ is 0, i.e., c is a root of

$$a^2X^2 + (-2a^{q+1} + 4b^{1+q})X + a^{2q} = 0. \quad (3.11)$$

Similar to the proof of Lemma 3.3, it has two solutions in $\mathbb{F}_{q^2}^*$. By Lemma (2.7), its solutions are $(q-1)$ -st power if and only if its discriminant $16b^{2(q+1)}\kappa(a,b)$ is 0 or a nonsquare of \mathbb{F}_q^* . Since $a^{q+1} \neq b^{q+1}$, we have $\kappa(a,b) \neq 0$. Therefore, $n_1 = 0$ or 2 according as $\kappa(a,b)$ is a square or nonsquare of \mathbb{F}_q^* . The claims in (1) and (2) now follows.

Suppose that q is even. The equation (3.10) has a repeated root if and only if its coefficient of X is 0, i.e., $a^q = ac$. It follows that $c = a^{q-1}$, and so $n_1 = 1$. The claim in (3) then follows. This completes the proof. \square

Let $N_{a,b}$ be the number of triples $(s, t, r) \in S \times T_1 \times \mathbb{F}_{q^2}^*$ such that (3.3) holds. Then $N_{b,a}$ is the number of triples such that (3.4) holds. We are now ready to compute $N_{a,b} + N_{b,a}$. Let \square (resp. \blacksquare) be the set of nonzero squares and nonsquares of \mathbb{F}_q . For a property P , we define $[[P]] := 1$ or 0 according as P holds or not.

Lemma 3.8. *Take notation as above. We have*

$$N_{a,b} = \begin{cases} (q-1) \cdot \left(\frac{q-1}{2} + [[\kappa(a,b) \in \square]] - [[\kappa(b,a) \in \square]] \right), & \text{if } q \text{ is odd;} \\ \frac{q}{2}(q-1), & \text{if } q \text{ is even.} \end{cases}$$

Proof. We first consider the case q is odd. Take a triple $(s, t, r) \in S \times T_1 \times \mathbb{F}_{q^2}^*$ such that (3.3) holds. By the analysis preceding Lemma 3.3, the value of t is uniquely determined by r and s by (3.5), and (3.6) should have two solutions in S , i.e., $r \in R_2$. By Lemma 3.5, we have $r^{q-1} + a^{q-1} \neq 0$. By Lemma 3.6, an element r such that $r^{q-1} + a^{q-1} \neq 0$ is in R_2 if and only if $\kappa(b,a) \in \square$.

We now reverse the above arguments. Take $r \in R_2$ such that $r^{q-1} + a^{q-1} \neq 0$. The two solutions s_1, s_2 of (3.6) are both in S , and $t_i = ar^{-1} - br^{-q}s_i^{-q}$, $i = 1, 2$, are in T by Lemma 3.5. By (2) of Lemma 3.4, exactly one of t_i 's is in T_1 , say, t_1 . Then (s_1, t_1, r) is a solution to (3.3). Therefore, $N_{a,b} = |R_2| - (q-1)[[\kappa(b,a) \in \square]]$, where the latter term corresponds to the $q-1$ r 's such that $r^{q-1} + a^{q-1} = 0$. By Lemma 3.7, we have $|R_2| = (q-1) \cdot \left(\frac{q-1}{2} + [[\kappa(a,b) \in \square]] \right)$. To sum up, we have

$$N_{a,b} = (q-1) \cdot \left(\frac{q-1}{2} + [[\kappa(a,b) \in \square]] \right) - (q-1)[[\kappa(b,a) \in \square]].$$

This completes the proof of the case q is odd. By the same argument, we get $N_{a,b} = |R_2|$ in the case q is even. This completes the proof. \square

Corollary 3.9. *For $f_{a,b} \in \text{GL}(V)$ with $ab \neq 0$, its multiplicity in $\tilde{A} \cdot \tilde{D}$ equals $q(q-1)$ or $(q-1)^2$ according as q is even or not.*

Proof. By our analysis following Lemma 3.2, this number equals the number of triples $(s, t, r) \in S \times T_1 \times \mathbb{F}_{q^2}^*$ such that (3.3) or (3.4) holds. It equals $N_{a,b} + N_{b,a}$, so the claim follows from Lemma 3.8. \square

By combining Lemma 3.2 and Corollary 3.9, we see that $\tilde{A} \cdot \tilde{D} = \lambda(q - 1) \cdot \text{GL}(V)$, where $\lambda = q$ or $q - 1$ according as q is even or odd. By taking quotient by the center, we conclude that Theorem 1.1 holds.

Acknowledgement. This work was supported by National Natural Science Foundation of China under Grant No. 11771392.

References

- [1] N. Biggs. Perfect codes in graphs. *J. Combin. Theory Ser. B*, 15:289–296, 1973.
- [2] J. Chen, Y. Wang, and B. Xia. Characterization of subgroup perfect codes in Cayley graphs. *Disc. Math.*, 343:111813, 2020.
- [3] L.E. Dickson. *Linear groups: with an exposition of the Galois field theory*. Teubner, Leipzig, 1901.
- [4] G. Etienne. Perfect codes and regular partitions in graphs and groups. *European J. Combin.*, 8:139–144, 1987.
- [5] H.M. Green and M.W. Liebeck. Some codes in symmetric and linear groups. *Disc. Math.*, 343(8):111719, 2020.
- [6] H. Huang, B. Xia, and S. Zhou. Perfect codes in Cayley graphs. *SIAM J. Disc. Math.*, 32:548–559, 2018.
- [7] O.H. King. The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, pages 29–56. Cambridge Univ. Press, Cambridge, 2005.
- [8] J. Kratochvíl. Perfect codes over graphs. *J. Combin. Theory Ser. B*, 40:224–228, 1986.
- [9] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
- [10] X. Ma, G.L. Walls, K. Wang, and S. Zhou. Subgroup perfect codes in Cayley graphs. <https://arxiv.org/abs/1904.01858>.
- [11] S. Terada. Perfect codes in $\text{SL}(2, 2^f)$. *European J. Combin.*, 25:1077–1085, 2004.
- [12] J.H. van Lint. A survey of perfect codes. *Rocky Mountain J. Math.*, 5(2):199–224, 1975.